

# Retail sector

## Notable news & breaches

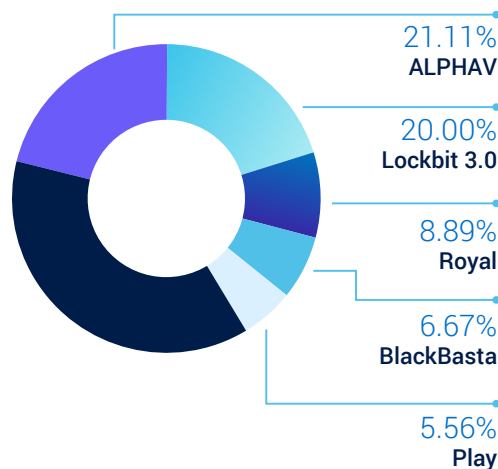
- Sur La Table released data breach notification, BlackBasta takes credit.
- Yum! Brands, the parent company of KFC, Taco Bell, and Pizza Hut, publicly disclosed Q1 breach of employee data.
- Aloha point of sale outage caused by ransomware incident.
- US man charged with hacking and fraud against sports betting website.
- Sysco, one of the largest distributors of foodservice products disclosed a breach in May that impacted over 125,000 individuals.

## Noteworthy threat actor

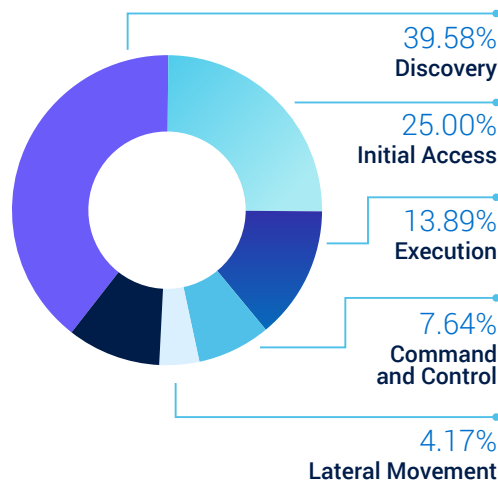
### FIN7

FIN7 is a financially-motivated group with a history of targeting the retail industry, especially in the United States. FIN7 has been notably active in Q2 2023, after a relatively quiet period over the previous year.

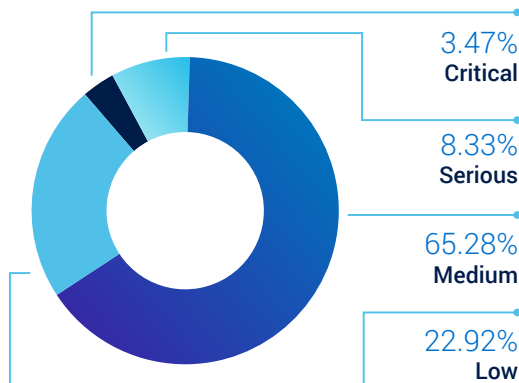
### Top ransomware



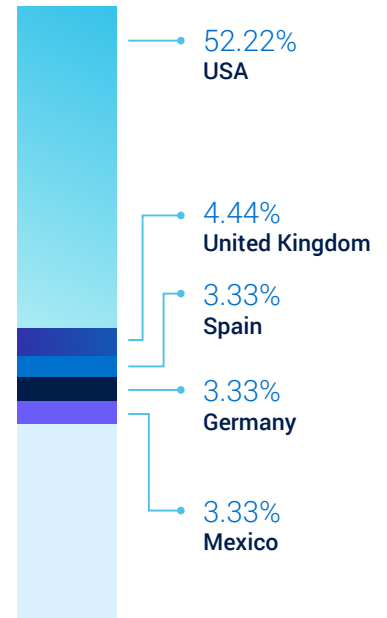
### Incident MITRE tactics



### Incident severity



### Ransomware victim locations



### Monthly victim trending

Ransomware	April	May	June
ALPHAV	7	4	8
Lockbit 3.0	8	5	5
Royal	7	1	0
BlackBasta	1	3	2
Play	1	3	1

## Recommendation

Where feasible, some form of dark web monitoring should be leveraged by retail organizations to monitor for brand impersonation and access for sale. This can help discover impersonation campaigns as well as remote and database access to e-commerce platforms for sale on forums such as Exploit.